ID: 756301
Sample Name: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Cookbook: default.jbs
Time: 00:29:09
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
PCAP (Network Traffic) 4
Memory Dumps 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe 12
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn 12
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn 12
C:\Users\user\AppData\Local\Temp\nsq493.tmp\System.dll 13
C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck 13
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3425316567-2969588382-3778222414-1001\1b1d0082738e9f9011266f86ab9723d2_11389406-0377-47ed-98c7-d564e683c6eb 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 16
Resources 16
Imports 16
Possible Origin 17
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 18
UDP Packets 19

DNS Queries 19
DNS Answers 20
HTTP Request Dependency Graph 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exePID: 4112, Parent PID: 4652 20
General 20
File Activities 21
Registry Activities 21
Analysis Process: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exePID: 7568, Parent PID: 4112 21
General 21
File Activities 21
File Created 21
File Written 22
File Read 22
Analysis Process: WerFault.exePID: 1144, Parent PID: 7568 22
General 22
File Activities 22
Disassembly 23

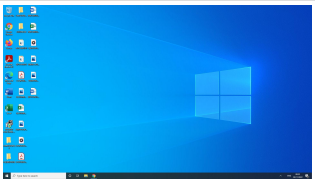
Windows Analysis Report

REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe

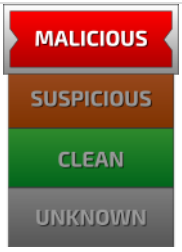
Overview

General Information

Sample Name:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Analysis ID:	756301
MD5:	b9f70f4146b8461..
SHA1:	97cb5de0e0cc2f...
SHA256:	ff235029990af04..
Infos:	



Detection



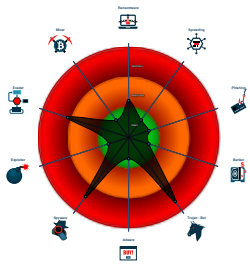
GuLoader, Lokibot

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi...
- Tries to harvest and steal Putty / W...
- Tries to detect Any.run
- Tries to harvest and steal ftp login c...
- Machine Learning detection for sam...
- Tries to harvest and steal browser in...
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe (PID: 4112 cmdline: C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe MD5: B9F70F4146B846179FA182AC868D0C15)
  - REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe (PID: 7568 cmdline: C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe MD5: B9F70F4146B846179FA182AC868D0C15)
    - WerFault.exe (PID: 1144 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7568 -s 1980 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.54385682867.00000000007CC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	
00000002.00000002.54387083303.00000000032D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.54201456373.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.11.20 - Destination IP: 157.245.36.27

Timestamp:	192.168.11.20157.245.36.2749838802021641 11/30/22-00:31:37.333969
SID:	2021641
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.11.20 - Destination IP: 157.245.36.27

Timestamp:	192.168.11.20157.245.36.2749838802024317 11/30/22-00:31:37.333969
SID:	2024317
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.11.20 - Destination IP: 157.245.36.27

Timestamp:	192.168.11.20157.245.36.2749838802024312 11/30/22-00:31:37.333969
SID:	2024312
Source Port:	49838
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Malware Analysis System Evasion

Tries to detect Any.run

Stealing of Sensitive Information

Yara detected Lokibot

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

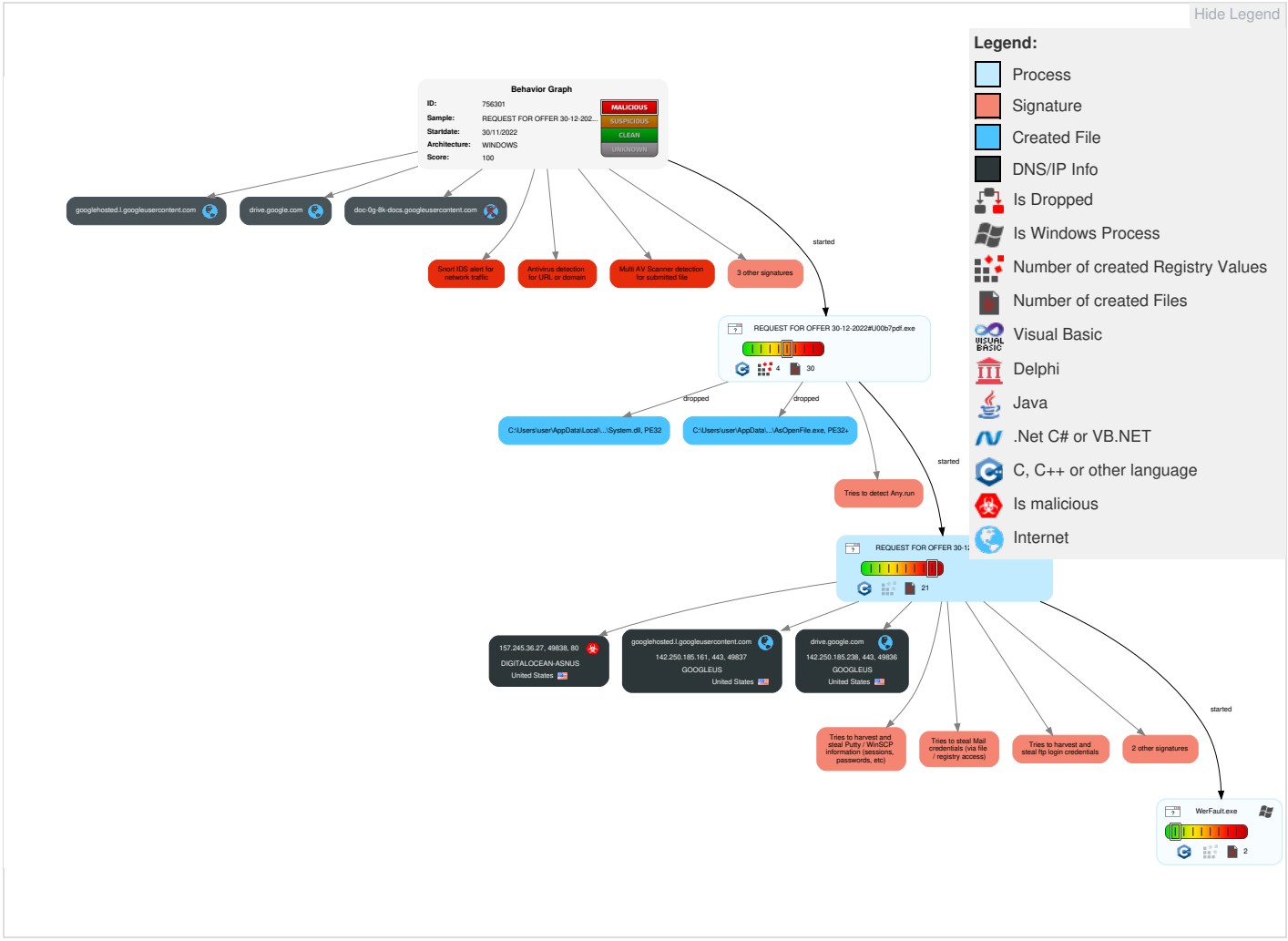
Remote Access Functionality

Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Windows Service	1 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 1 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	6 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

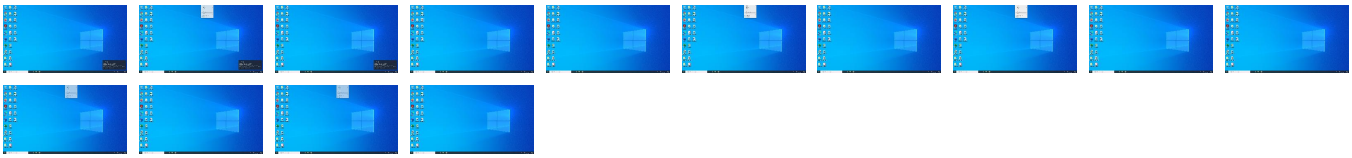
Behavior Graph

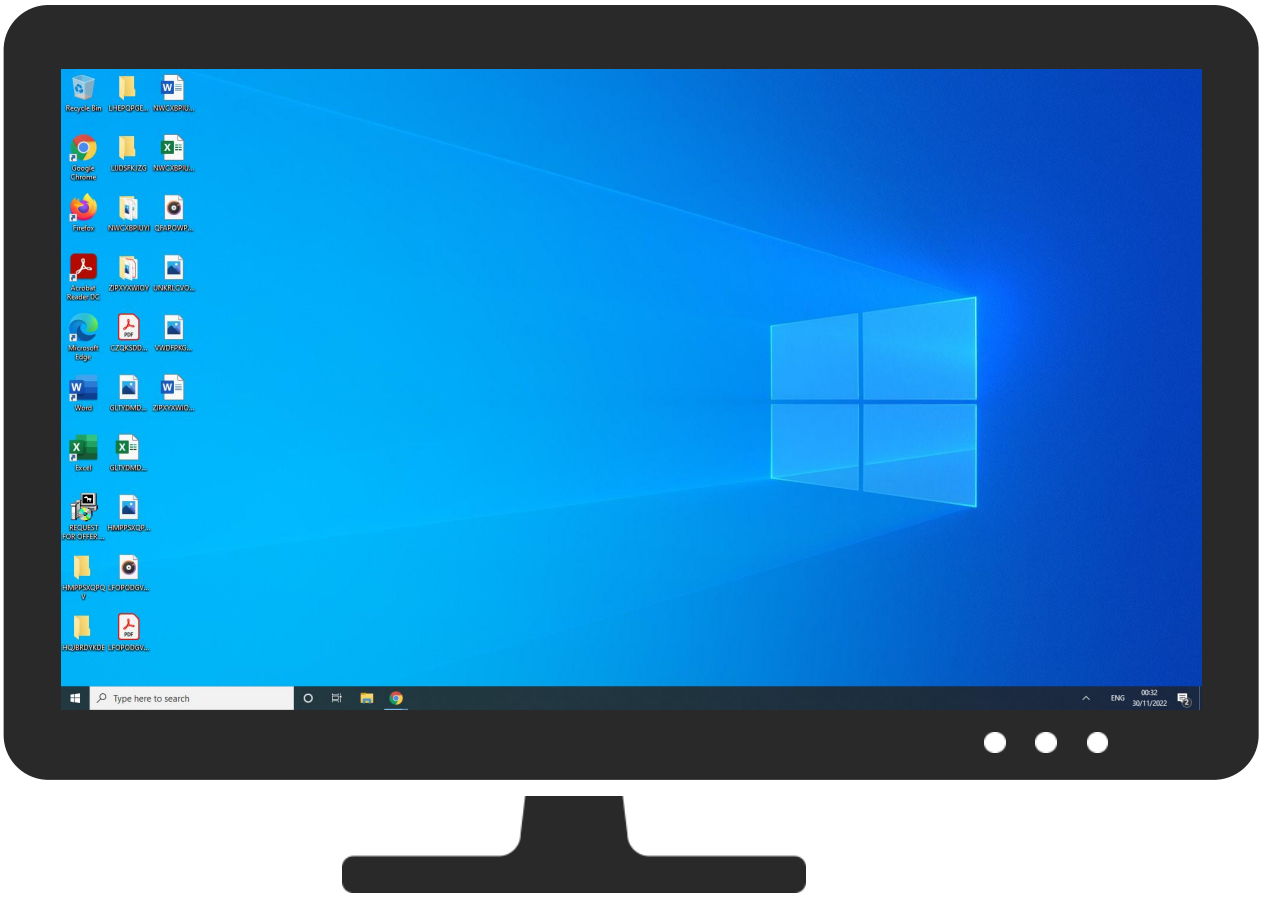


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	18%	ReversingLabs		
REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsq493.tmp\System.dll	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://157.245.36.27/~dokterpol/?page=2874	100%	Avira URL Cloud	malware	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Virustotal		Browse
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.161	true	false		high
doc-0g-8k-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

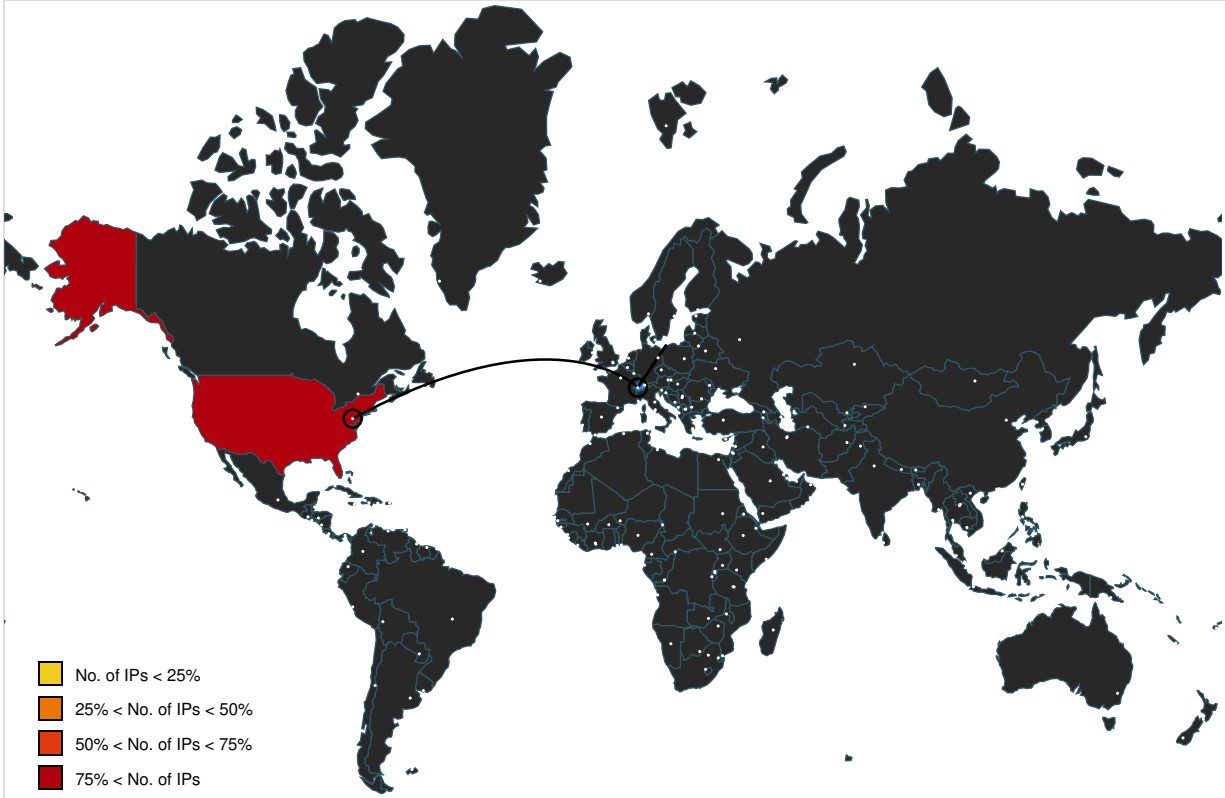
Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0g-8k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/65eu063p0f9eoc2qkjfmonuuk5gkqmq4/1669764675000/03238822727237126472/*/1ZppbncXCwboWfcBo0A5zlqzevMjFwzpW?e=download&uuid=c4bc146b-22c6-4e17-89b8-c96a6eb96fab	false		high
http://157.245.36.27/~dokterpol/?page=2874	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-0g-8k-docs.googleusercontent.com/%%doc-0g-8k-docs.googleusercontent.com	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54391896205.0000000001901000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54203683114.0000000005F2000.00000008.00000001.01000000.00000006.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://drive.google.com/	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54391638858.0000000018E5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54204236542.0000000000649000.00000008.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000003.54356841847.0000000001984000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54392074084.0000000001919000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54204236542.0000000000649000.00000008.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54203683114.0000000005F2000.00000008.00000001.01000000.00000006.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://doc-0g-8k-docs.googleusercontent.com/)	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54391896205.0000000001901000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54204053166.0000000000626000.00000008.00000001.01000000.00000006.sdmp	false		high
http://www.gopher.ftp://ftp.	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000001.54204236542.0000000000649000.00000008.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-0g-8k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/65eu063p	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000003.54362021539.0000000001943000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000003.54356420593.0000000001943000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54392699460.0000000001943000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54392074084.0000000001919000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0g-8k-docs.googleusercontent.com/	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000003.54362021539.0000000001943000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54391896205.0000000001901000.00000004.00000020.00020000.00000000.sdmp, REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe, 00000005.00000002.54392699460.0000000001943000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
157.245.36.27	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
142.250.185.238	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756301
Start date and time:	2022-11-30 00:29:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/6@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.1% (good quality ratio 29.4%) • Quality average: 88.5% • Quality standard deviation: 21.7%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\AsOpenFile.exe

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38632
Entropy (8bit):	5.840976252158136
Encrypted:	false
SSDEEP:	768:tba0g4rhVUkxIlaPrd6cMCP1diTLmz1BeeKH2X98VwhH:HPUkxIlaPrsCPXK6z1Bee3+k
MD5:	ED609F8F09DE8AAA4F8CFF0285E0420A
SHA1:	A7ADE9EB5BD4BAEFAB796C1D6EA92417F1396135
SHA-256:	2488796ACE769813C729198CFD9E3C9D0A512168301D387BE569F2557C683821
SHA-512:	32F080433C121FE1970BBB82911024A389E43B8B6BA059931FF0F3AFA4096BE79660C6DC9C1E027C21692D320F95896B0211C9FA0997AEC30F7A373382443FF2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..r..r..r..4r..r..s..r..s..r..s..r..s..r..r..r..s..rp.s..rp.Xr..r.0r..rp.s..rR ich..r.....PE..d.....a.....#.....^.....@.....Vo.... .....N.....h....p..L....x.....B..p.....@D.. (...@C.....0.....text..... ..`.rdata..*....0...0..."....@..@.data.....`.....R.....@....pdata..L....p.....T.....@..@.rsrc...h..... ...X.....@..@..... .....

C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\Tusindtallig.Syn

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	29309
Entropy (8bit):	**7.9930541941014255**
Encrypted:	**true**
SSDEEP:	768:E49NB/CsjPddY0nfj1fIXSgH0uO7wt1WayrQ0bThetG:nlCsxfVIXHH2wOfKG
MD5:	849FDC040AA117FC8B8AC03C745C690D
SHA1:	831EE9C0B27F05069A323940A7C581CA21C9BE68
SHA-256:	3C6382D1FD4C832B2BBD7CDD2508DDAA80BF40D17732C8B17C31D70CED631A79
SHA-512:	A5F45B85DAD9FD26B7B111F402467D33B92E01F9C13CD4C2932FA53617746C246393BFEF020DAEE78F4C4515BABA2B50461DA761607CD97A200B3E2206BB08A 6
Malicious:	false
Reputation:	low
Preview:	...'.A&:}.....Y8.)..rRqi....t.b.&..K1....vy}5j.....=.f.(.....3C....p+,+.`Y[]..'u.1.].].0..?KP..F.v\..M...(.V.M..^D".3.r..t....9\.N...R..6..K..S.....o|.^Z b....C.G$.s(k^...m...r.L70.m.2q' .7.%*t..5u..d.#..T.,....%..5O?..".G._.(._V.....7e.``..r....~u.A..-o.7.{.....9.T<.+.H...u.}P..:.....p..t...^...D.....#..0....j.?D.rG.."....C.....QP.....+.A..=...|.X..J.w(..V.....>{8.... .7. 2m...>..;=.-....Qq...cx.=.....3..m.x.#..../.....3.w.@Rd.rVt..Q.v..1LW`]'..Bs.{.....5....J...t..o..1..M.....H,(ugAw.....C.]...J.y...<~(u.....|..Y....B...}....(cn.....Gc..|.6x6w.....HD. ...GV.....r....u\.....^Po.._|]R.....R...|. LH....Z/}(st..0..F..L...J.G 5|.0t.q.x..m..W..X.k..=..k.+.a..U...r..f..|<O...t.vN.)..>t..J.j....J.'..OR.-.S..cU....?X.....L!.....3....I...a..A.[c.,....2....p.~..!%..m.2.....[=.....r.n.6.....G...1...lqV..fn..j...E..[.....>.CZHT.....w..~7<=.....<8e..l.p..Q...f.....qD..]Xh..LA...J.....7.....O..

C:\Users\user\AppData\Local\Folkedansens\Suffigere\Glaucophane\prowl.Dgn

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	141909
Entropy (8bit):	7.124693631306355
Encrypted:	false

SSDEEP:	3072:COxlLD2mpgf8pOxNjQzNUflgAG63+OAyam6kxnv:COxlmcg5EzuNG6MyaJSv
MD5:	0A951AA33DE8994CBE161F0E07F169B8
SHA1:	38033C58EEFF600D22A068F1A7F599646BDFDD1E
SHA-256:	4A98204499C5BA9F9518D6A7EF078A5A5F0B82173919E9A5D41179172BD28F60
SHA-512:	F9BE445FDBD89EB0F5CACBB325D89E89755906F1DADE3A7E32593E4ADFCBFF2C8927350226BB8FD0238B4F8F72377F757ADCDAFE20C7FA2FF41C4A14814D8 A27
Malicious:	false
Reputation:	low
Preview:	.T.....i.. ..YA..^..;;..3Gn._+.P.a1TG...$;....r..K...8.W..gS..9j.t...j y._........e.....[z......Ae.8/..f........B..).. ....o..-...7.Qf......B..e...f....L..2B..!..a....-.F..ooo ooooooooooooooooooooooooooooooooooooo..c.B......JV.XS...B.....f.r...=..U...f....'.5~.......... ....9x...f....:.e...67..N...!.f...f....9$}17...2/. .LPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPf......

C:\Users\user\AppData\Local\Temp\nsq493.tmp\System.dll

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8QIl975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0
SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092 CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......1...u.u.u...s.u.a....r.!..q....t....t.Richu.........................PE..L.....MX.. ....!..... ....'.......0...............................`.......................................2.......0..P...........................P.......................................................0..X...........................text............ ........ .......... ..`.rdata..S....0.......$.............@..@.data...x....@.......(..............@....reloc..b....P.......*.............@..B... ....

C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3425316567-2969588382-3778222414-1001\1b1d0082738e9f9011266f86ab9723d2_11389406-0377-47ed-98c7-d564e683c6eb

Process:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.1262763721961973
Encrypted:	false
SSDEEP:	3:/lSllIEXln:AWE1
MD5:	D69FB7CE74DAC48982B69816C3772E4E
SHA1:	B1C04CDB2567DC2B50D903B0E1D0D3211191E065

SHA-256:	8CC6CA5CA4D0FA03842A60D90A6141F0B8D64969E830FC899DBA60ACB4905396
SHA-512:	7E4EC58DA8335E43A4542E0F6E05FA2D15393E83634BE973AA3E758A870577BA0BA136F6E831907C4B30D587B8E6EEAFA2A4B8142F49714101BA50ECC294DDB0
Malicious:	false
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.875386203366202
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
File size:	194987
MD5:	b9f70f4146b846179fa182ac868d0c15
SHA1:	97cb5de0e0cc2f53cd73552f9d5b4381ab5a5907
SHA256:	ff235029990af0449ce8f82c5546dfe37170d5e27ce1a22b0a43965a980344be
SHA512:	2cc45205394074ddf9a5481a81b89582d84d42a34023329e06cf589c455c2fef144905362b5d1001e26026480d490304b6ac96526ab32f5344b1706d98ceff48
SSDEEP:	3072:MRD+3q3NxPTNuY/bQZFler2MUPaSa1y8XKdV06k55ohchNqV3AzlbEnJZGqItyWJ:mwq3NpNSFleCMUPVaidHXMNqwlInJ0q8
TLSH:	A714125533E0C523CAF202702DBB652F9EE9A642E262FF131360AF9D7D56307864C356
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40344a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x584DCA38 [Sun Dec 11 21:50:48 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4ea4df5d94204fc550be1874e1b77ea7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi

Instruction
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007FED94512513h
push ebx
call 00007FED9451566Ch
cmp eax, ebx
je 00007FED94512509h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FED945155E6h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FED945124ECh
push ebp
push 00000009h
call 00007FED9451563Eh
push 00000007h
call 00007FED94515637h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007FED94515220h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FED9451520Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x69000	0xb48	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x3e000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x69000	0xb48	0xc00	False	0.4228515625	data	4.372183800985918	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x691c0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x694a8	0x100	data	English	United States
RT_DIALOG	0x695a8	0x11c	data	English	United States
RT_DIALOG	0x696c8	0xc4	data	English	United States
RT_DIALOG	0x69790	0x60	data	English	United States
RT_GROUP_ICON	0x697f0	0x14	data	English	United States
RT_MANIFEST	0x69808	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, WaitForSingleObject, GetCurrentProcess, CompareFileTime, GlobalUnlock, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, lstrcpyW, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GlobalFree, GlobalAlloc, GetShortPathNameW, SearchPathW, lstrcmpiW, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, lstrcmpW, GetDiskFreeSpaceW, lstrlenW, lstrcpynW, GetExitCodeProcess, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, MulDiv, MultiByteToWideChar, lstrlenA, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW

DLL	Import
USER32.dll	GetSystemMenu, SetClassLongW, IsWindowEnabled, EnableMenuItem, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, wsprintfW, ScreenToClient, GetWindowRect, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, LoadImageW, SetTimer, SetWindowTextW, PostQuitMessage, ShowWindow, GetDlgItem, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegDeleteKeyW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges, RegOpenKeyExW, RegEnumValueW, RegDeleteValueW, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

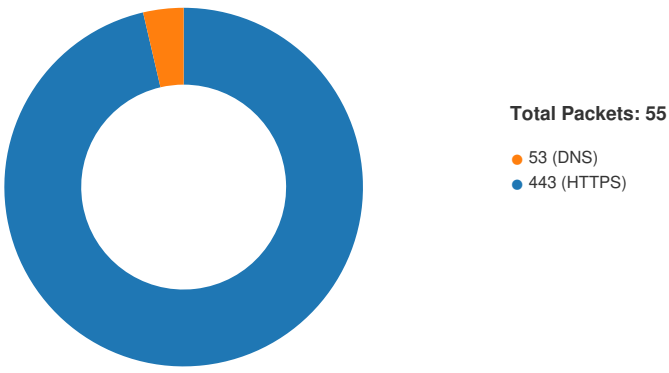
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20157.245.36.2749838802021641 11/30/22-00:31:37.333969	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49838	80	192.168.11.20	157.245.36.27
192.168.11.20157.245.36.2749838802024317 11/30/22-00:31:37.333969	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49838	80	192.168.11.20	157.245.36.27
192.168.11.20157.245.36.2749838802024312 11/30/22-00:31:37.333969	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49838	80	192.168.11.20	157.245.36.27

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:31:35.123769999 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.123786926 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.124044895 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.137362957 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.137372017 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.172802925 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.173031092 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.173213005 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.173417091 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.173674107 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.302972078 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.304261923 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.304462910 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.308245897 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.348491907 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.606657982 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.606863022 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.606874943 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.607048035 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.608479023 CET	49836	443	192.168.11.20	142.250.185.238
Nov 30, 2022 00:31:35.608555079 CET	443	49836	142.250.185.238	192.168.11.20
Nov 30, 2022 00:31:35.794887066 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.794929981 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.795146942 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.795490026 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.795507908 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.858731031 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.858937979 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.859126091 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.860200882 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.860357046 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.860357046 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.864449978 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.864485025 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.864960909 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:35.865122080 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.865542889 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:35.912424088 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.193646908 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.193851948 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.194185972 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.194263935 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.194359064 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.194547892 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.195283890 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.195485115 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.195549965 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.195982933 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.196171045 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.196225882 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.196439028 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.198167086 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.198345900 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.198385954 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.198849916 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.201076031 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.201406956 CET	49837	443	192.168.11.20	142.250.185.161

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:31:36.203979969 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.204233885 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.204291105 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.204576015 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.204622984 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.204778910 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.204869986 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.204936028 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.204979897 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.205188990 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.205256939 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.205456018 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.205496073 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.205528975 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.205698967 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.205699921 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.206115007 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.206336021 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.206392050 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.206670046 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.206896067 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.207021952 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.207073927 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.207273006 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.207426071 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.207664013 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.207719088 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.207990885 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.208270073 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.208506107 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.208565950 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.208812952 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.209053993 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.209290028 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.209343910 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.209602118 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.209661961 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.209861040 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.209897995 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.210105896 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.210390091 CET	443	49837	142.250.185.161	192.168.11.20
Nov 30, 2022 00:31:36.210585117 CET	49837	443	192.168.11.20	142.250.185.161
Nov 30, 2022 00:31:36.210622072 CET	443	49837	142.250.185.161	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:31:35.102749109 CET	49240	53	192.168.11.20	1.1.1.1
Nov 30, 2022 00:31:35.111932993 CET	53	49240	1.1.1.1	192.168.11.20
Nov 30, 2022 00:31:35.755490065 CET	53919	53	192.168.11.20	1.1.1.1
Nov 30, 2022 00:31:35.793382883 CET	53	53919	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:31:35.102749109 CET	192.168.11.20	1.1.1.1	0x6df6	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:31:35.755490065 CET	192.168.11.20	1.1.1.1	0x3147	Standard query (0)	doc-0g-8k-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false

DNS Answers

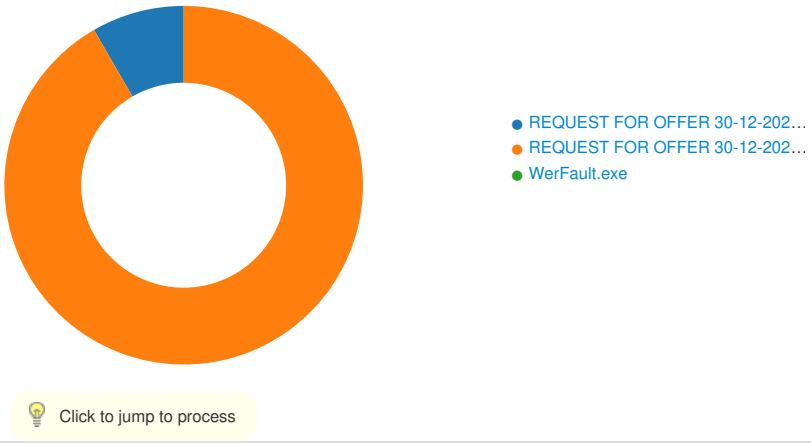
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:31:35.111932993 CET	1.1.1.1	192.168.11.20	0x6df6	No error (0)	drive.google.com		142.250.185.238	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:31:35.793382883 CET	1.1.1.1	192.168.11.20	0x3147	No error (0)	doc-0g-8k-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:31:35.793382883 CET	1.1.1.1	192.168.11.20	0x3147	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.161	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-0g-8k-docs.googleusercontent.com
- 157.245.36.27

Statistics

Behavior



System Behavior

Analysis Process: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe PID: **4112**, Parent PID: **4652**

General

Target ID:	2
Start time:	00:31:01

Start date:	30/11/2022
Path:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Imagebase:	0x400000
File size:	194987 bytes
MD5 hash:	B9F70F4146B846179FA182AC868D0C15
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000002.00000002.54385682867.00000000007CC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.54387083303.00000000032D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe PID: **7568**, Parent PID: **4112**

General

Target ID:	5
Start time:	00:31:18
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\REQUEST FOR OFFER 30-12-2022#U00b7pdf.exe
Imagebase:	0x400000
File size:	194987 bytes
MD5 hash:	B9F70F4146B846179FA182AC868D0C15
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000000.54201456373.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1680720	InternetOpenUrlA
C:\Users\user\AppData\Roaming\5D4ACB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	3920	success or wait	1	40415C	ReadFile

Analysis Process: WerFault.exe PID: **1144**, Parent PID: **7568**

General

Target ID:	8
Start time:	00:31:37
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7568 -s 1980
Imagebase:	0x520000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly